DETAILED ACTION

1. This Office Action is in response to the most recent papers filed on 4/19/2006.

2. Claims 68-83 are rejected.

Information Disclosure Statement

1. The information disclosure statement filed 12/14/2005 fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each cited foreign patent document; each non-patent literature publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed.

2. Foreign Patent Document WO 03/014935 A has not been considered because a copy of the Foreign Patent Document was not found in the current application file.

Oath/Declaration

1. The oath or declaration is defective. A new oath or declaration in compliance with 37 CFR 1.67(a) identifying this application by application number and filing date is required. See MPEP §§ 602.01 and 602.02.

The oath or declaration is defective because:
It does not identify the citizenship of each inventor.

Specifically Ryoji Kato's Citizenship was left blank.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 68-83 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 68 starts by stating "A system for supporting Hierarchical Mobile IP version 6 (HMIPv6) service for a mobile node, comprising:"

If the limitations are part of the system they have patentable weight if they are part of the mobile node they do not as the limitations are then only being applied to an object of intended use. Assuming that applicant intends for the limitations to be part of the claimed system Examiner suggests amending the starting lines of claim 68 to read "A system for supporting Hierarchical Mobile IP version 6 (HMIPv6) service for a mobile node, said system comprising:".

Claim 77 starts by stating "An AAA server for supporting Hierarchical Mobile IP version 6 (HMIPv6) service for a mobile node, comprising"

If the limitations are part of the AAA server they have patentable weight if they are part of the mobile node they do not as the limitations are then only being applied to an object of intended use. Assuming that applicant intends for the limitations to be part of the claimed AAA server Examiner suggests amending the starting lines of claim 77 to read "An AAA server for supporting Hierarchical Mobile IP version 6 (HMIPv6) service for a mobile node, said AAA server comprising: ".

Claim 80 starts by stating "An AAA home network server (AAAh) for supporting Hierarchical Mobile IP version 6 (HMIPv6) service for a mobile node, comprising:"

If the limitations are part of the AAAh they have patentable weight if they are part of the mobile node they do not as the limitations are then only being applied to an object of intended use. Assuming that applicant intends for the limitations to be part of the claimed AAAh Examiner suggests amending the starting lines of claim 80 to read "An AAA home network server (AAAh) for supporting Hierarchical Mobile IP version 6 (HMIPv6) service for a mobile node, said AAAh comprising:".

Claim 83 starts by stating "A system for supporting Hierarchical Mobile IP version 6 (HMIPv6) service for a mobile node, further comprising".

As mentioned in the claims above if the limitations are part of the system they have patentable weight if they are part of the mobile node they do not as the limitations are then only being applied to an object of intended use.

In addition as this is the start of an independent claim there is a question to what is intended by the **further** comprising.

Examiner suggests amending the starting lines of claim 83 to read "A system for supporting Hierarchical Mobile IP version 6 (HMIPv6) service for a mobile node, said system ~~further~~ comprising".

Claims 69-76 are dependents of claim 68.

Claims 78-79 are dependents of claim 77.

Claims 81-82 are dependents of claim 80.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 59-83 are rejected as being non-statutory as they are neither tied to a specific machine nor do they provide a transformation of mater.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 59-63, 68-72 & 77-82 are rejected under 35 U.S.C. 102(b) as being anticipated by Hierarchical MIPv6 mobility management (HMIPMM).

As per Claim 59: HMIPMM teaches: A method of supporting Hierarchical Mobile IP version 6 (HMIPv6) service for a mobile node using an AAA infrastructure to bootstrap the HMIPv6 service said method comprising the steps of:

- said AAA infrastructure assigning an appropriate Mobility Anchor Point (MAP) to the mobile node for the HMIPv6 service

(HMIPMM, Page 4, Lines 6-9 "A MAP may also interact with the AAA protocol to perform key distribution during handoffs and eliminate the need for re-authentication as explained in chapter 11.").

(HMIPMM, Page 19, Lines 26-34 "HMIPv6 does not introduce more security problems than Mobile IPv6. The IPSec SA are created by using the home address of the mobile host.

A mobile host has to register with its home agent and with the Mobility Anchor Point. All registration messages between the MN and the MAP have to be authenticated. This means that the mobile host has to share an authentication key (private or public) with all MAPs it may visit. These keys can be pre-installed manually or obtained dynamically via IKE or AAA servers.").

- transferring HMIPv6-related information required for authenticating and authorizing the mobile node for the HMIPv6 service with the assigned MAP over said AAA infrastructure

(HMIPMM, Page 20, Lines 1-4 "One example of the interaction between a MAP and the AAA infrastructure can be seen when considering the handoff scenario. A MAP can store the MN's security credentials after the MN is allowed network access by the AAA infrastructure.").

As per Claim 60: The rejection of claim 59 is incorporated and further HMIPMM teaches:

- an AAA server of said AAA infrastructure assigns an appropriate MAP to the mobile node for the HMIPv6 service

(HMIPMM, Page 19, Lines 26-34 "HMIPv6 does not introduce more security problems than Mobile IPv6. The IPSec SA are created by using the home address of the mobile host.

A mobile host has to register with its home agent and with the Mobility Anchor Point. All registration messages between the MN and the MAP have to be authenticated. This means that the mobile host has to share an authentication key (private or public) with all MAPs it may visit. These keys can be pre-installed manually or obtained dynamically via IKE or AAA servers.").

As per Claim 61: The rejection of claim 60 is incorporated and further HMIPMM teaches:

- the mobile node is roaming in a visited network, further comprising the step of an AAA visited network server (AAAv) assigning a MAP in the visited network to the mobile node based on a policy of the visited network operator

(HMIPMM, Page 19, Lines 29-34 "A mobile host has to register with its home agent and with the Mobility Anchor Point. All registration messages between the MN

and the MAP have to be authenticated. This means that the mobile host has to share an authentication key (private or public) with all MAPs it may visit. These keys can be pre-installed manually or obtained dynamically via IKE or AAA servers.").

(HMIPMM, Page 18, Lines 7-30 "HMIPv6 provides a very flexible mechanism for local mobility management within a visited network. As explained earlier a MAP can exist on any level in a hierarchy including the AR. Several MAPs can be located within a hierarchy independantly of each other. In addition, overlapping MAP domains are also allowed and recommended. Both static and dynamic hierarchies are supported for either mode of operation. Hence the discussion below is independant of the MAP's mode of operation. When the MN receives a router Advertisement including a MAP option, it should perform actions according to the following movement detection mechanisms. In a Hierarchical Mobile IP network such as the one described in this draft, the MN SHOULD be:

- "Eager" to perform new bindings
- "Lazy" in releasing existing bindings

The above means that the MN will register with any "new" MAP advertised by the AR (Eager). The method by which the MN determines whether the MAP is a "new" MAP is described above. The MN should not release existing bindings until it no longer receives its MAP option or the lifetime of its existing binding expires (Lazy). This Eager-Lazy approach described above will assist in providing a fallback mechanism in case one of the MAP routers crash as it would reduce the time it takes for a MN to inform its CNs and HA about its new COA.").

As per Claim 62: The rejection of claim 59 is incorporated and further HMIPMM teaches:

- an AAA infrastructure component of the home network generating credential-related data for security association between the mobile node and the assigned MAP and sending said credential-related data to the MAP, the AAA infrastructure home network component generating information for finalizing the security association or the MAP responding with information for finalizing the security association to the AAA infrastructure home network component, which sends HMIPv6 authorization information to the mobile node over the AAA infrastructure

(HMIPMM, Page 19, Lines 26-34 "HMIPv6 does not introduce more security problems than Mobile IPv6. The IPSec SA are created by using the home address of the mobile host.

A mobile host has to register with its home agent and with the Mobility Anchor Point. All registration messages between the MN and the MAP have to be authenticated. This means that the mobile host has to share an authentication key (private or public) with all MAPs it may visit. These keys can be pre-installed manually or obtained dynamically via IKE or AAA servers.").

As per Claim 63: The rejection of claim 59 is incorporated and further HMIPMM teaches:

- transferring HMIPv6-related information over said AAA infrastructure for establishing a HMIPv6 security association between the mobile node and the assigned MAP and for establishing a HMIPv6 binding for the mobile node, and wherein HMIPv6-related information for HMIPv6 binding is transferred in the same round trip as HMIPv6-related information for HMIPv6 security association

(HMIPMM, Page 19, Lines 26-34 "HMIPv6 does not introduce more security problems than Mobile IPv6. The IPSec SA are created by using the home address of the mobile host.

A mobile host has to register with its home agent and with the Mobility Anchor Point. All registration messages between the MN and the MAP have to be authenticated. This means that the mobile host has to share an authentication key (private or public) with all MAPs it may visit. These keys can be pre-installed manually or obtained dynamically via IKE or AAA servers.").

As per Claim 68: HMIPMM teaches: A system for supporting Hierarchical Mobile IP version 6 (HMIPv6) service for a mobile node, comprising:

- an AAA infrastructure component operable for assigning an appropriate Mobility Anchor Point (MAP) to the mobile node for the HMIPv6 service

(HMIPMM, Page 4, Lines 6-9 "A MAP may also interact with the AAA protocol to perform key distribution during handoffs and eliminate the need for re-authentication as

explained in chapter 11.").

(HMIPMM, Page 19, Lines 26-34 "HMIPv6 does not introduce more security problems than Mobile IPv6. The IPSec SA are created by using the home address of the mobile host.

A mobile host has to register with its home agent and with the Mobility Anchor Point. All registration messages between the MN and the MAP have to be authenticated. This means that the mobile host has to share an authentication key (private or public) with all MAPs it may visit. These keys can be pre-installed manually or obtained dynamically via IKE or AAA servers.").

- means for transferring HMIPv6-related information required for authenticating and authorizing the mobile node for the HMIPv6 service with the assigned MAP over said AAA infrastructure

(HMIPMM, Page 20, Lines 1-4 "One example of the interaction between a MAP and the AAA infrastructure can be seen when considering the handoff scenario. A MAP can store the MN's security credentials after the MN is allowed network access by the AAA infrastructure.").

As per Claim 69: The rejection of claim 68 is incorporated and further HMIPMM teaches:

- said AAA infrastructure component is an AAA server that is operable for assigning an appropriate MAP to the mobile node for the HMIPv6 service

(HMIPMM, Page 19, Lines 26-34 "HMIPv6 does not introduce more security problems than Mobile IPv6. The IPSec SA are created by using the home address of the mobile host.

A mobile host has to register with its home agent and with the Mobility Anchor Point. All registration messages between the MN and the MAP have to be authenticated. This means that the mobile host has to share an authentication key (private or public) with all MAPs it may visit. These keys can be pre-installed manually or obtained dynamically via IKE or AAA servers.").

As per Claim 70: The rejection of claim 69 is incorporated and further HMIPMM teaches:

- the mobile node is roaming in a visited network, and an AAA visited network server (AAAv) is operable for assigning a MAP in the visited network to the mobile node based on a policy of the visited network operator

(HMIPMM, Page 19, Lines 29-34 "A mobile host has to register with its home agent and with the Mobility Anchor Point. All registration messages between the MN and the MAP have to be authenticated. This means that the mobile host has to share an authentication key (private or public) with all MAPs it may visit. These keys can be pre-installed manually or obtained dynamically via IKE or AAA servers.").

(HMIPMM, Page 18, Lines 7-30 "HMIPv6 provides a very flexible mechanism for local mobility management within a visited network. As explained earlier a MAP can exist on any level in a hierarchy including the AR. Several MAPs can be located within a hierarchy independantly of each other. In addition, overlapping MAP domains are also allowed and recommended. Both static and dynamic hierarchies are supported for either mode of operation. Hence the discussion below is independant of the MAP's mode of operation. When the MN receives a router Advertisement including a MAP option, it should perform actions according to the following movement detection mechanisms. In a Hierarchical Mobile IP network such as the one described in this draft, the MN SHOULD be:

- "Eager" to perform new bindings
- "Lazy" in releasing existing bindings

The above means that the MN will register with any "new" MAP advertised by the AR (Eager). The method by which the MN determines whether the MAP is a "new" MAP is described above. The MN should not release existing bindings until it no longer receives its MAP option or the lifetime of its existing binding expires (Lazy). This Eager-Lazy approach described above will assist in providing a fallback mechanism in case one of the MAP routers crash as it would reduce the time it takes for a MN to inform its CNs and HA about its new COA.").

As per Claim 71: The rejection of claim 68 is incorporated and further HMIPMM teaches:

- an AAA infrastructure component of the home network comprises: means for generating credential-related data for security association between the mobile node and the assigned MAP; means for sending said credential-related data to the assigned MAP; means for receiving information from the MAP for finalizing the security association; and, means for sending HMIPv6 authorization information to the mobile node over the AAA infrastructure

(HMIPMM, Page 19, Lines 26-34 "HMIPv6 does not introduce more security problems than Mobile IPv6. The IPSec SA are created by using the home address of the mobile host.

A mobile host has to register with its home agent and with the Mobility Anchor Point. All registration messages between the MN and the MAP have to be authenticated. This means that the mobile host has to share an authentication key (private or public) with all MAPs it may visit. These keys can be pre-installed manually or obtained dynamically via IKE or AAA servers.").

As per Claim 72: The rejection of claim 68 is incorporated and further HMIPMM teaches:

- means for transferring HMIPv6-related information over said AAA infrastructure for establishing a HMiPv6 security association between the mobile node and the assigned MAP and for establishing a HMIPv6 binding for the mobile node, and

wherein HMIPv6-related information for HMIPv6 binding is transferred in the same round trip as HMIPv6-related information for HMIPv6 security association

(HMIPMM, Page 19, Lines 26-34 "HMIPv6 does not introduce more security problems than Mobile IPv6. The IPSec SA are created by using the home address of the mobile host.

A mobile host has to register with its home agent and with the Mobility Anchor Point. All registration messages between the MN and the MAP have to be authenticated. This means that the mobile host has to share an authentication key (private or public) with all MAPs it may visit. These keys can be pre-installed manually or obtained dynamically via IKE or AAA servers.").

As per Claim 77: HMIPMM teaches: An AAA server for supporting Hierarchical Mobile IP version 6 (HMIPv6) service for a mobile node, comprising

- means for assigning a Mobility Anchor Point (MAP) to the mobile node for the HMIPv6 service

(HMIPMM, Page 4, Lines 6-9 "A MAP may also interact with the AAA protocol to perform key distribution during handoffs and eliminate the need for re-authentication as explained in chapter 11.").

(HMIPMM, Page 19, Lines 26-34 "HMIPv6 does not introduce more security problems than Mobile IPv6. The IPSec SA are created by using the home address of the mobile host.

A mobile host has to register with its home agent and with the Mobility Anchor Point. All registration messages between the MN and the MAP have to be authenticated. This means that the mobile host has to share an authentication key (private or public) with all MAPs it may visit. These keys can be pre-installed manually or obtained dynamically via IKE or AAA servers.").

(HMIPMM, Page 20, Lines 1-4 "One example of the interaction between a MAP and the AAA infrastructure can be seen when considering the handoff scenario. A MAP can store the MN's security credentials after the MN is allowed network access by the AAA infrastructure.").

As per Claim 78: The rejection of claim 77 is incorporated and further HMIPMM teaches:

- the mobile node is roaming in a visited network, and said AAA server is an AAA visited network server (AAAv) operable for assigning a MAP in the visited network

(HMIPMM, Page 19, Lines 29-34 "A mobile host has to register with its home agent and with the Mobility Anchor Point. All registration messages between the MN and the MAP have to be authenticated. This means that the mobile host has to share an authentication key (private or public) with all MAPs it may visit. These keys can be pre-installed manually or obtained dynamically via IKE or AAA servers.").

(HMIPMM, Page 18, Lines 7-30 "HMIPv6 provides a very flexible mechanism for local mobility management within a visited network. As explained earlier a MAP can exist on any level in a hierarchy including the AR. Several MAPs can be located within a hierarchy independantly of each other. In addition, overlapping MAP domains are also allowed and recommended. Both static and dynamic hierarchies are supported for either mode of operation. Hence the discussion below is independant of the MAP's mode of operation. When the MN receives a router Advertisement including a MAP option, it should perform actions according to the following movement detection mechanisms. In a Hierarchical Mobile IP network such as the one described in this draft, the MN SHOULD be:

- "Eager" to perform new bindings
- "Lazy" in releasing existing bindings

The above means that the MN will register with any "new" MAP advertised by the AR (Eager). The method by which the MN determines whether the MAP is a "new" MAP is described above. The MN should not release existing bindings until it no longer receives its MAP option or the lifetime of its existing binding expires (Lazy). This Eager-Lazy approach described above will assist in providing a fallback mechanism in case one of the MAP routers crash as it would reduce the time it takes for a MN to inform its CNs and HA about its new COA.").

As per Claim 79: The rejection of claim 77 is incorporated and further HMIPMM teaches:

- said AAA server is an AAA home network server (AAAh) operable for assigning a MAP in the home network of the mobile node

(HMIPMM, Page 8, Lines 16-20 "This section outlines the extensions proposed to the BU option used by the MN in MIPv6. A new flag is added: the M flag that indicates MAP registration. When a MN registers with the MAP, the M flag MUST be set to distinguish this registration from a Home Registration or a BU being sent to a CN.").

As per Claim 80: HMIPMM teaches: An AAA home network server (AAAh) for supporting Hierarchical Mobile IP version 6 (HMIPv6) service for a mobile node, comprising:

- means for generating credential-related data for security association between the mobile node and a Mobility Anchor Point (MAP) assigned by an AAA infrastructure component; means for sending said credential-related data to the assigned MAP; means for receiving information from the MAP for finalizing the security association; and, means for sending HMIPv6 authorization information including security association information to the mobile node

(HMIPMM, Page 19, Lines 26-34 "HMIPv6 does not introduce more security problems than Mobile IPv6. The IPSec SA are created by using the home address of the mobile host.

A mobile host has to register with its home agent and with the Mobility Anchor Point. All registration messages between the MN and the MAP have to be authenticated. This means that the mobile host has to share an authentication key (private or public) with all MAPs it may visit. These keys can be pre-installed manually or obtained dynamically via IKE or AAA servers.").

As per Claim 81: The rejection of claim 80 is incorporated and further HMIPMM teaches:

- said mobile node is roaming in a visited network, and said means for sending HMIPv6 authorization information is operable for sending the information over an AAA infrastructure linking the visited network with the home network of the mobile node

(HMIPMM, Page 19, Lines 29-34 "A mobile host has to register with its home agent and with the Mobility Anchor Point. All registration messages between the MN and the MAP have to be authenticated. This means that the mobile host has to share an authentication key (private or public) with all MAPs it may visit. These keys can be pre-installed manually or obtained dynamically via IKE or AAA servers.").

(HMIPMM, Page 18, Lines 7-30 "HMIPv6 provides a very flexible mechanism for local mobility management within a visited network. As explained earlier a MAP can exist on any level in a hierarchy including the AR. Several MAPs can be located within a hierarchy independantly of each other. In addition, overlapping MAP domains are also

allowed and recommended. Both static and dynamic hierarchies are supported for either mode of operation. Hence the discussion below is independant of the MAP's mode of operation. When the MN receives a router Advertisement including a MAP option, it should perform actions according to the following movement detection mechanisms. In a Hierarchical Mobile IP network such as the one described in this draft, the MN SHOULD be:

- "Eager" to perform new bindings
- "Lazy" in releasing existing bindings

The above means that the MN will register with any "new" MAP advertised by the AR (Eager). The method by which the MN determines whether the MAP is a "new" MAP is described above. The MN should not release existing bindings until it no longer receives its MAP option or the lifetime of its existing binding expires (Lazy). This Eager-Lazy approach described above will assist in providing a fallback mechanism in case one of the MAP routers crash as it would reduce the time it takes for a MN to inform its CNs and HA about its new COA.").

As per Claim 82: The rejection of claim 80 is incorporated and further HMIPMM teaches:

- said AAA home network server is configured for receiving, from the assigned MAP, information for finalizing the security association as well as binding address information, and said means for sending HMIPv6 authorization

information over the AAA infrastructure is configured for sending HMIPv6 authorization information including MAP assignment information, binding address information and security association information to the mobile node

(HMIPMM, Page 19, Lines 26-34 "HMIPv6 does not introduce more security problems than Mobile IPv6. The IPSec SA are created by using the home address of the mobile host.

A mobile host has to register with its home agent and with the Mobility Anchor Point. All registration messages between the MN and the MAP have to be authenticated. This means that the mobile host has to share an authentication key (private or public) with all MAPs it may visit. These keys can be pre-installed manually or obtained dynamically via IKE or AAA servers.").

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 64-67 & 73-76 are rejected under 35 U.S.C. 103(a) as being unpatentable over HMIPMM in view of United States Patent Application Publication No.: US 3003/0199104 A1 (Kakemizu et al.).

As per Claim 64: The rejection of claim 59 is incorporated and further HMIPMM does not explicitly teach the following limitations however Kakemizu et al. in analogous art does teach the following limitations:

- the mobile node is roaming in a visited network, and HMIPv6-related authentication and authorization information is transferred between the mobile node and an AAA home network server (AAAh) within an authentication protocol in an end-to-end procedure transparent to the visited network

(Kakemizu et al., Paragraphs [0015]-[0016], "According to the present invention, in a network in which service information is delivered using a protocol for authentication of a terminal, an address assignment protocol is linked with the authentication protocol. Therefore, service information can be delivered to the router device corresponding to a terminal in the address assignment procedure for the terminal.

If the request for an address is made using the ICMPv6, and the request for authentication is made using the AAA protocol, then the ICMPv6, which is an address assignment protocol in the IPv6, is linked with the AAA protocol for authentication of the terminal. Accordingly, the service information can be delivered to the router device corresponding to the IPv6 in the address assignment procedure for the IPv6 terminal.").

(Kakemizu et al., Paragraph [0110], "FIG. 5 shows a basic sequence of delivering service control information. It is described based on the network shown in FIG. 2. In this example, the service control information about the IPv6 host 11 is delivered to the edge node 22. The IPv6 host 11 is authenticated by the AAA server (AAAH) 1. The service

control information about the IPv6 host 11 is assumed to be stored in a database (SPDB) 51 accessible by the AAA server 1.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Kakemizu et al. in to the method of HMIPMM in order to have underlying systems to run the MIPv6 extensions on.

As per Claims 65-66: The rejection of claim 64 is incorporated and further the examiner is giving official notice that the Extensible Authentication Protocol (EAP) was a well know authentication protocol in the art at the time of invention was made. It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the use of the Extensible Authentication Protocol (EAP) in to HMIPMM and Kakemizu et al.'s method in order to have the use of already existing authentication protocols.

As per Claim 67: The rejection of claim 64 is incorporated and further HMIPMM does not explicitly teach the following limitations however Kakemizu et al. in analogous art does teach the following limitations:

- the assigned MAP is located in the visited network, and HMIPv6-related information is transferred between the mobile node and the AAA home network server (AAAh) within said authentication protocol, and HMIPv6-related

information is transferred between the AAAh and the assigned MAP in the visited network within an AAA framework protocol application

(Kakemizu et al., Paragraphs [0015]-[0016], "According to the present invention, in a network in which service information is delivered using a protocol for authentication of a terminal, an address assignment protocol is linked with the authentication protocol. Therefore, service information can be delivered to the router device corresponding to a terminal in the address assignment procedure for the terminal.

If the request for an address is made using the ICMPv6, and the request for authentication is made using the AAA protocol, then the ICMPv6, which is an address assignment protocol in the IPv6, is linked with the AAA protocol for authentication of the terminal. Accordingly, the service information can be delivered to the router device corresponding to the IPv6 in the address assignment procedure for the IPv6 terminal.").

(Kakemizu et al., Paragraph [0110], "FIG. 5 shows a basic sequence of delivering service control information. It is described based on the network shown in FIG. 2. In this example, the service control information about the IPv6 host 11 is delivered to the edge node 22. The IPv6 host 11 is authenticated by the AAA server (AAAH) 1. The service control information about the IPv6 host 11 is assumed to be stored in a database (SPDB) 51 accessible by the AAA server 1.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Kakemizu et al. in to the method of HMIPMM in order to have underlying systems to run the MIPv6 extensions on.

As per Claim 73: The rejection of claim 68 is incorporated and further HMIPMM does not explicitly teach the following limitations however Kakemizu et al. in analogous art does teach the following limitations:

- the mobile node is roaming in a visited network, and HMIPv6-related authentication and authorization information is transferred between the mobile node and an AAA home network server (AAAh) within an authentication protocol in an end-to-end procedure transparent to the visited network

(Kakemizu et al., Paragraphs [0015]-[0016], "According to the present invention, in a network in which service information is delivered using a protocol for authentication of a terminal, an address assignment protocol is linked with the authentication protocol. Therefore, service information can be delivered to the router device corresponding to a terminal in the address assignment procedure for the terminal.

If the request for an address is made using the ICMPv6, and the request for authentication is made using the AAA protocol, then the ICMPv6, which is an address assignment protocol in the IPv6, is linked with the AAA protocol for authentication of the terminal. Accordingly, the service information can be delivered to the router device corresponding to the IPv6 in the address assignment procedure for the IPv6 terminal.").

(Kakemizu et al., Paragraph [0110], "FIG. 5 shows a basic sequence of delivering service control information. It is described based on the network shown in FIG. 2. In this example, the service control information about the IPv6 host 11 is delivered to the edge node 22. The IPv6 host 11 is authenticated by the AAA server (AAAH) 1. The service

control information about the IPv6 host 11 is assumed to be stored in a database (SPDB) 51 accessible by the AAA server 1.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Kakemizu et al. in to the method of HMIPMM in order to have underlying systems to run the MIPv6 extensions on.

As per Claims 74-75: The rejection of claim 73 is incorporated and further the examiner is giving official notice that the Extensible Authentication Protocol (EAP) was a well know authentication protocol in the art at the time of invention was made. It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the use of the Extensible Authentication Protocol (EAP) in to HMIPMM and Kakemizu et al.'s method in order to have the use of already existing authentication protocols.

As per Claim 76: The rejection of claim 73 is incorporated and further HMIPMM does not explicitly teach the following limitations however Kakemizu et al. in analogous art does teach the following limitations:

- the assigned MAP is located in the visited network, and HMIPv6-related information is transferred between the mobile node and an AAA home network server (AAAh) within said authentication protocol, and HMIPv6-related

information is transferred between the AAAh and the assigned MAP in the visited network within an AAA framework protocol application

(Kakemizu et al., Paragraphs [0015]-[0016], "According to the present invention, in a network in which service information is delivered using a protocol for authentication of a terminal, an address assignment protocol is linked with the authentication protocol. Therefore, service information can be delivered to the router device corresponding to a terminal in the address assignment procedure for the terminal.

If the request for an address is made using the ICMPv6, and the request for authentication is made using the AAA protocol, then the ICMPv6, which is an address assignment protocol in the IPv6, is linked with the AAA protocol for authentication of the terminal. Accordingly, the service information can be delivered to the router device corresponding to the IPv6 in the address assignment procedure for the IPv6 terminal.").

(Kakemizu et al., Paragraph [0110], "FIG. 5 shows a basic sequence of delivering service control information. It is described based on the network shown in FIG. 2. In this example, the service control information about the IPv6 host 11 is delivered to the edge node 22. The IPv6 host 11 is authenticated by the AAA server (AAAH) 1. The service control information about the IPv6 host 11 is assumed to be stored in a database (SPDB) 51 accessible by the AAA server 1.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Kakemizu et al. in to the method of HMIPMM in order to have underlying systems to run the MIPv6 extensions on.

10. Claim 83 is rejected under 35 U.S.C. 103(a) as being unpatentable over HMIPMM.

As per Claim 83: HMIPMM teaches: A system for supporting Hierarchical Mobile IP version 6 (HMIPv6) service for a mobile node, further comprising

- means for transferring HMIPv6-related authentication and authorization information between the mobile node and an AAA home network server over an AAA infrastructure for authenticating and authorizing the mobile node for HMIPv6 service,

(HMIPMM, Page 4, Lines 6-9 "A MAP may also interact with the AAA protocol to perform key distribution during handoffs and eliminate the need for re-authentication as explained in chapter 11.").

(HMIPMM, Page 19, Lines 26-34 "HMIPv6 does not introduce more security problems than Mobile IPv6. The IPSec SA are created by using the home address of the mobile host.

A mobile host has to register with its home agent and with the Mobility Anchor Point. All registration messages between the MN and the MAP have to be authenticated. This means that the mobile host has to share an authentication key (private or public) with all MAPs it may visit. These keys can be pre-installed manually or obtained dynamically via IKE or AAA servers.").

(HMIPMM, Page 20, Lines 1-4 "One example of the interaction between a MAP and the AAA infrastructure can be seen when considering the handoff scenario. A MAP can store the MN's security credentials after the MN is allowed network access by the AAA infrastructure.").

HMIPMM does not explicitly teach the following limitation:

- transferring HMIPv6- related authentication and authorization information in an Extensible Authentication Protocol (EAP) said HMIPv6-related information being incorporated as additional data in the EAP protocol stack

However examiner is giving official notice that the Extensible Authentication Protocol (EAP) was a well know authentication protocol in the art at the time of invention was made. It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the use of the Extensible Authentication Protocol (EAP) in to HMIPMM's method in order to have the use of already existing authentication protocols.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BENJAMIN A. KAPLAN whose telephone number is (571)-270-3170. The examiner can normally be reached on 7:30 a.m. - 5:00 p.m. E.S.T..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Benjamin Kaplan

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434